Call for views on the journalism code of practice

Key themes and summary of responses

October 2021

ico.
Information Commissioner's Office

Contents

1. How we have responded to your feedback: key points 3
2. Summary of responses and ICO comment 6
2.1. Key themes 7
2.1.1. General scope 7
2.1.2. Structure 8
2.1.3. Key principles 9
2.1.4. Content 10
2.1.4.1. Storage limitation 10
2.1.4.2. Accuracy 11
2.1.4.3. Accountability 11
2.1.4.4. Security 12
2.1.4.5. Fairness and lawfulness 12
2.1.5. Individual rights 14
2.1.6. Digital change 15
2.1.7. The special purposes exemption 16
2.1.8. Legal defences 17
2.1.9. Third parties 17
2.1.10. Supervision and review process 18
2.1.11. Case studies 19

1. How we have responded to your feedback: key points

Defining journalism

Our code explains that 'journalism' is not limited to professional journalists. It may also include other members of the public publishing information. The code sets out factors to help you to consider whether an activity is journalism. It also considers the circumstances in which online services may be engaging in journalism.

The special purposes exemption

This exemption is the main provision in data protection law protecting journalism. Our code provides greater clarity on its application, including:

- the meaning of 'with a view to publication' and how this applies to complaints about journalism;
- what it means to have a reasonable belief that publication is in the public interest; and
- how to record decisions proportionately.

Data protection impact assessments (DPIAs)

You need a DPIA for any type of processing likely to result in a high risk to people. Our code explains how to do this proportionately. You do not need to carry out a DPIA for every story likely to involve high risk processing. A more general DPIA or series of DPIAs that apply to the overall type of processing, eg special investigations journalism, is likely to be sufficient as long as it covers the processing you carry out, identifies the risks and how you mitigate these.

Dealing with personal data lawfully

Our code includes guidance on the lawful bases journalists are most likely to use: consent and legitimate interests. It also includes guidance on the additional conditions for processing special category or criminal offence data. In particular, the guidance covers:

- what 'manifestly made public by the data subject' means; and
- how organisations may use the 'reasons of substantial public interest' condition to disclose information to journalists in connection with unlawful

acts and dishonesty.

Criminal allegations

Our code provides guidance when considering the publication of criminal allegations. It explains that although the general starting point is that a suspect has a reasonable expectation of privacy regarding investigations, there may be a reason why an expectation of privacy is not reasonable in the circumstances or why an originally reasonable expectation may no longer exist. There may also be limited circumstances where the public interest may justify identifying a suspect. There must be a strong public interest for identifying a suspect, as the harmful consequences are likely to be substantial.

Providing privacy information to people

Generally, people have the right to be informed about the collection and use of their personal data. This is known as privacy information. The code explains that if you collect personal data from someone directly, there are no exceptions from this requirement. If you collect personal data from other sources, you do not need to provide information if it would:

- involve disproportionate effort;
- seriously impair your objectives; or
- mean that meeting your objectives is impossible.

Where necessary, you may also consider the special purposes exemption if you believe these provisions would be incompatible with journalism.

Making sure personal data is accurate in the digital age

Our code includes guidance on:

- conducting reasonable accuracy checks, including in urgent scenarios and more challenging circumstances such as live broadcasting;
- distinguishing between facts and opinions and reflecting the context; and
- dealing with sources of information, particularly online sources such as social media.

The code also explains when you may use inaccurate personal data in stories without breaching the accuracy data protection principle.

Retaining research and contact details

Our code acknowledges that research and contact details are vital to journalism. We know that you may wish to keep them indefinitely or for a long, unspecified period of time. Data protection law does not impose a specific time limit. The key point is that you are able to justify why keeping the information is proportionate. This may be difficult to know in the context of journalism, but you should still consider how likely it is that you will need to use the information in future.

Roles and responsibilities

When a third party is involved in processing personal data, you should decide whether they are a controller or a processor. Our code explains these different roles, how to identify them and what responsibilities are attached. It explains good practice when sharing personal data, including what to consider when third parties provide you with personal data that you want to use for journalism.

Individual data protection rights

People have a number of different rights that they can exercise concerning their personal data. Our code explains what you need to consider in the context of journalism.

For example, people may sometimes ask you to erase their personal data. This is not an absolute right and it only applies in certain circumstances. The right to erasure does not apply if the processing is necessary to exercise the right to freedom of expression. There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a weighty factor in favour of not erasing personal data from archives.

The protection of sources

Our code explains that that protection of confidential sources is fundamental to a free press. Legislation reflects this. For example, under section 10 of the Contempt of Court Act 1981, a publisher cannot be compelled to reveal the source of published information unless a court considers it to be in the interests of justice, national security or the prevention of crime. It is therefore very unlikely that you would be required to disclose information about confidential sources in response to a SAR from another individual.

2. Summary of responses and ICO comment

In a call for views that closed in May 2019, we consulted on the development of the journalism Code of Practice (the code). We must produce this code in accordance with section 124 of the Data Protection Act 2018 (DPA 2018). We are required to produce practical guidance to support people to understand their legal obligations and good practice in the context of data protection and journalism.

In particular, the call for views sought views on:

- our existing guidance regarding journalism and using it as the basis for a new code;
- the code's structure;
- the key areas we should address in the code;
- changes in data protection law, key legal cases and other developments since we published our earlier guidance; and
- useful case studies or scenarios to include in the code.

Overall, we received 40 responses to the call for views. We broke down the responses as follows:

- Media organisations – 15;
- Trade associations – 6;
- Regulator – 1;
- Organisations representing data subjects – 1;
- Academics – 2;
- Individuals acting in a professional capacity – 7;
- Individual acting in a private capacity – 5;
- Other – 3.

The responses to the call for views helped us to consider the scope and structure of the code. It was helpful to hear about the themes that stakeholders urged us to reflect in the code. Responses also helped us to understand key concerns regarding:

- the special purposes exemption for journalism;
- data protection principles; and
- individual rights.

Respondents were keen for the code to reflect practical scenarios, the digital age and up-to-date case law. One practical scenario that respondents wanted to understand more about is the role and responsibilities of third parties processing personal data for journalism. Respondents wanted greater clarity over how third parties may supply information to journalists in the public interest.

We are very grateful to everyone who took the time to respond to this call for views. Ultimately, we want to create a code that is helpful to you and your

feedback is fundamental to our considerations. Whilst we cannot reply to each respondent, we have analysed the key themes raised and included our response. Where applicable, we explain how the draft code addresses the issues raised.

The call for views represented the first stage of the consultation process. We are now running a public consultation for 12 weeks alongside other stakeholder engagement.

2.1. Key themes

2.1.1. General scope

Respondents said the code should generally align with other media codes.

It would be helpful for the code to elaborate further on what constitutes journalism. 'Journalism' should be interpreted broadly. For example, the code should explain that journalism can apply to:

- 'citizen journalism';
- bloggers in some circumstances; and
- those wishing to supply personal data to journalists, such as whistle-blowers.

The code should reflect, as much as possible, the different parts of the industry. This includes television, rather than focusing on print media. This would result in a wider range of examples and application.

In the context of television, scripted and non-scripted programming pose different challenges. It would be helpful if the code could touch upon the extent to which other 'special purposes' apply when producing documentaries or programmes.

It is important to recognise the dynamic nature of journalism. The code should take into account that media organisations vary in:

- size;
- structure;
- staff;
- location;
- resources; and
- audience.

The code would be likely to stand the best chance of staying relevant if it was flexible. It also needs to be realistic about how organisations make decisions in very fast-paced and competitive environments that need to produce contemporaneous news.

The code should seek to recognise relevant legal judgements more fully and address the key areas where issues commonly arise for journalists. It would also be helpful to refer to the rulings of the Independent Press Standards Organisation (IPSO) to help journalists balance competing interests.

ICO response

The code is limited to data protection in the context of journalism, not industry standards more generally. However, we believe that our code is well-aligned and complementary to industry codes (see our impact assessment). We reviewed industry codes and talked to representatives from IPSO, the BBC, OFCOM and IMPRESS. As appropriate, we include references and links to industry codes and guidance, although these do not form part of the code itself.

The code refers to existing case law and, like our older media guidance, explains that journalism should be interpreted broadly. This includes professionals as well as non-professionals, such as citizen journalists. Although this code is focused on the 'special purposes' of journalism, it also explains that the special purposes more broadly, including art and literature, is likely to cover the entire output of the print or broadcast media.

We want the code to be of practical use to all parts of the industry. The code also includes guidance on topics that broadcasters told us would be particularly helpful to them. For example, there is guidance about consent and written releases, and on dealing with the accuracy principle when broadcasting live.

In the context of the special purposes exemption, the code acknowledges the practical reality that journalists 'on the ground' often make decisions at a fast pace. It is clear that controllers may delegate responsibility. The code explains that it is important to consider the overall risks and put clear policies and procedures in place to support this.

We have updated our guidance to highlight key privacy case law using examples. We explain how the case law applies practically in common areas that journalists are likely to encounter.

2.1.2. Structure

Respondents said the current structure of our guidance is helpful and represents a good starting point.

While a layered approach continues to be important, the core building blocks of the code should be relevant to anyone processing personal data for the purposes of journalism. This is unlike ICO's current media guidance, which is split to target 'day-to-day journalism' and those who require more detailed or complex guidance.

The structure for each section could be:

- scope;
- standards (possibly split into default provisions and then criteria for exemption);
- processes (which would necessarily be highly contextual given that this depends on the organisation);
- supervision; and
- dispute resolution.

The code should be in 'bite-sized' chunks that could be easily updated at a later stage as required.

ICO response

We used our existing guidance as the starting point when developing this code, but we did make some structural changes.

We recognise that journalism is often fast-paced and competitive. There are also a wide range of different organisations and individuals engaged in journalism. The code itself is generally applicable to anyone processing personal data for the purposes of journalism. However, we want to support day-to-day journalism.

The code is split into 10 main sections, which we intend to form the basis for a 'quick guide'. This would support day-to-day journalism and smaller organisations. Each section explains what the law says, why it is important to comply and how to comply effectively.

We welcome further feedback to help us to consider the code's structure and its practical use. This is part of the public consultation.

2.1.3. Key principles

Respondents said the code should reflect the importance of, and strong public interest in, the right to freedom of expression and information across all forms of journalism, and explain this more fully. The code should robustly deal with the protection of journalistic sources.

The code should be proportionate in its approach. Whilst recognising the strong need to protect personal data, this needs to be balanced against the potential harm that could be caused if data protection is applied too onerously.

The code should clearly recognise that the ICO is not a specialist media regulator and allow for editorial independence. It should be clear that the ICO's role is not to substitute its own views for those of journalists.

ICO response

The code explains how we had regard to the special public interest in journalism and why journalism is important to our democracy. The code also explains why it is necessary to balance this with the right to privacy.

We took a proportionate and flexible approach, tailoring our guidance in the code to reflect the public interest journalism serves and the fast-paced, competitive nature of the work. We explained that data protection is generally risk-based. This is fundamental to all the principles, including accountability which concerns putting in place appropriate data protection measures.

In the context of journalism, we explained that it is not necessary to conduct a data protection impact assessment (DPIA) for every story for example. Recording decision-making about whether publication is in the public interest when applying the special purposes exemption for journalism is another area where there is appropriate flexibility, depending on the circumstances.

As with the older media guidance, the code clearly acknowledges that the code is not about media standards generally. It is limited to journalism in the context of data protection.

Drawing on relevant case law, the code is clear that the special purposes exemption is designed to respect the independent judgement and expertise of journalists on the public interest. It reiterates that it is not the ICO's role to substitute its own view in place of journalists. The ICO's role is only to consider whether the belief was objectively reasonable.

2.1.4. Content

We received a number of comments from respondents about the content we should include in the code. We grouped the main comments under the relevant data protection principle.

2.1.4.1. Storage limitation

It is very important for the code to be clear about data retention. In particular, it should address the protection of archive material and journalistic research including contact information.

ICO response

The code recognises the importance of research, background information and contacts for the purposes of journalism. It explains that a proportionate, risk-based and flexible approach is appropriate. For example, journalists can store data without a specific story in mind, but they should still periodically review it. Where possible, journalists should be able to justify why they are keeping

personal data, via an appropriate retention schedule.

The code is clear that individuals have a right to erasure in certain circumstances. However, this right is not absolute and there is protection where the processing is necessary to exercise the right to freedom of expression and information. In practice, it is unlikely that a news archive would erase personal data, because of the important public interest role archives serve. Where necessary, the special purposes exemption for journalism is also available.

2.1.4.2. Accuracy

Principles derived from defamation law may be helpful in this context. An example is the importance of context in assessing accuracy and the protection of statements of opinion.

The code should be clear that the principle of accuracy does not mean erasing older stories as a story develops.

ICO response

In line with the UK GDPR, the code is clear that journalists should clearly distinguish between fact and opinion when reporting information about individuals. It also highlights that it may be necessary to provide appropriate clarification or context to avoid compromising accuracy. For example, the text should support headlines about individuals.

The code makes clear that the accuracy principle does not mean that journalists must erase older stories as a story develops. There is a strong public interest in preserving news archives. It is generally good practice to make a record of mistakes, however, in the form of corrections. Where necessary, the special purposes exemption for journalism is also available.

2.1.4.3. Accountability

The code should distinguish between recording what is essential and what is preferable. A prescriptive 'one size fits all' approach to recording and evidence would not be appropriate. Journalists should not always be required to keep contemporaneous records in all cases in order to rely on the special purposes exemption.

It is important to be realistic about record-keeping in view of journalism's fast pace and competitive nature. This is heightened by digital change and the speed of publication. DPIAs in particular must be proportionate.

The ICO should consider organisations involved in journalism training and education.

ICO response

The code reflects that accountability is a key principle of data protection. The principle itself is flexible and scalable because it is inherently risk-based. This means that organisations and individuals must assess the appropriate data protection measures in the circumstances, depending on what they do with personal data. There is appropriate flexibility for DPIAs, for example, as mentioned above. The code refers to the ICO's separate Accountability Framework to provide more support.

In the context of the special purposes exemption, the code is explicit that journalists do not necessarily need to record the decision to rely on the special purposes exemption. However, doing this helps to demonstrate compliance effectively. The code recognises that urgency and the public interest may mean that it is not always possible to keep a contemporaneous note. Journalists should then consider recording it after the decision. It may be difficult to subsequently recall factual details, if challenged, when there is no record. Simple checklists and templates can assist and the level of risk is a helpful guiding factor.

We continue to engage stakeholders through the public consultation period, including training providers.

2.1.4.4. Security

Issues include:

- data in transit or data stored in a cloud;
- software for handling personal data; and
- personal devices.

ICO response

The code refers to the ICO's separate Accountability Framework that includes measures and steps that organisations and individuals can take to keep personal data secure. The ICO also has also published separate guidance on cloud computing.

The code highlights that security policies and procedures should consider the heightened security risks arising from the work that journalists do, such as risks concerning remote working. We also have guidance on bringing your own device.

2.1.4.5. Fairness and lawfulness

There is concern about unexpected and sudden invasions of privacy in particular such as:

- the use of long-lens photography;

- 'door-stepping';
- 'micro-phone-in-face' reporting; and
- drones capturing personal data from people's homes or gardens.

Further guidance would be helpful about processing children's personal data and that of other vulnerable individuals, especially in sensitive locations such as hospitals or prisons. It would be helpful to explain the relevance of the ICO's Age Appropriate Design Code in relation to children accessing journalistic websites.

Generally, it is important for the code to recognise the close connection between data protection law and other laws. This includes laws that protect individuals from unlawful processing, such as defamation law and laws about the misuse of private information.

Guidance on the use of special category and criminal offence data in the context of journalism would be welcome. In particular, clarity on the 'manifestly made public' condition, when individuals engage in criminal behaviour.

The code should consider the public interest in circumstances where there are only allegations or suspicions of wrong-doing. It would be helpful to consider the broader implications of the legal case brought by Cliff Richard against the BBC in particular.

It would be helpful to clarify the legal bases or conditions that journalists could rely on in certain scenarios. Information on how these may vary depending on different genres of television, methods of filming or filming in a public place would also be helpful.

Changes on consent introduced by the UK GDPR are important. A particular challenge, for example, is protecting producers from withdrawal of consent given the cost of filming and production.

ICO response

The code covers covert surveillance, subterfuge and similar intrusive methods. It explains that it is likely journalists would need to rely on the special purposes exemption for journalism if deploying such methods. It also says that it may be more difficult to justify in the public interest because of the particularly intrusive nature of this activity, especially if dealing with special category or criminal offence data.

The code refers to the need to consider the sensitivity of children's personal data where relevant. It also highlights detailed separate guidance on children's personal data and the Age Appropriate Design Code (AADC). We have also published separate FAQs on the AADC for the digital news industry.

The code briefly explains the broader context of privacy law such as the tort of misuse of private information and defamation. We also discuss how compliance

with this code may help the media to comply with other privacy laws. We use examples from the broader area of privacy law where relevant to data protection.

The code provides guidance on the lawful bases most likely to be relevant in the context of journalism and how to approach the issue of criminal allegations. It also explains the application of the 'manifestly made public' condition regarding special category and criminal offence data.

Regarding consent, the code considers the scenario raised about withdrawal of consent for broadcasters relying on 'written releases' and offers practical guidance.

2.1.5. Individual rights

Respondents said the right to erasure may not be compatible with journalism. It would be helpful to understand when a correction rather than erasure is more appropriate.

There are similar concerns about the right to rectification. This should be confined to significant factual inaccuracies with latitude given for journalism. This right should not be applied to prevent journalistic enquiries.

There are concerns about dealing with subject access requests, especially when it undermines journalism. An example of this would be in relation to journalistic sources or disrupting investigations or publications.

There is also concern about notifying the public in line with the right to be informed. Organisations feel this could result in steps being taken to suppress an investigation or a story.

It would be helpful to clarify whether data portability meant personal data might need to be transferred to a competitor.

ICO response

The code makes clear that the right to erasure is not absolute and only applies in certain circumstances. It does not apply if the processing is necessary to exercise freedom of expression and information, so there is in-built protection for journalism. The code is also clear about the strong public interest in news archives, which is generally a weighty factor in favour of not erasing personal data from archives. Journalists could also apply the special purposes exemption where necessary.

The code covers the accuracy principle and the associated right to rectification. This requires reasonable steps to make sure personal data is accurate. This includes guidance on corrections. Accuracy is considered to be the hallmark of responsible journalism because it is usually difficult to argue that accuracy is

incompatible with journalism. It is therefore important in the context of journalism that reasonable action is taken when inaccuracies come to light.

We provide practical guidance in the code about dealing with subject access requests. This includes clarity on the strength of protection afforded to journalistic sources.

Transparent processing of personal data forms part of one of the key data protection principles, closely linked to lawfulness and fairness. The code includes guidance on the circumstances when organisations do not need to provide privacy information to individuals. It is clear that it is not always reasonable for journalists to notify an individual with privacy information. For example, this could undermine their journalistic purpose. If journalists do not consider that any of the exemptions apply, they may consider applying the special purposes exemption.

2.1.6. Digital change

Digital change is creating new challenges for journalists, for example:

- taking personal data from social media;
- the immediacy of publication on digital platforms;
- online archiving;
- responsibility for online 'below the line' comments;
- online harms; and
- the use of AI and the 'Internet of Things' to generate journalistic content.

ICO response

Increasing confidence in the processing of personal data in the digital age is one of our key objectives. We recognise that the pace of technological change means that much has changed since we last published guidance for the media in 2014.

While it is relatively straight-forward to recognise when media organisations, for example, are processing personal data for the purposes of journalism, other scenarios may require more consideration. We considered the code's application in the context of online services. We also explain how relevant factors can assist in identifying controllers processing personal data for the purposes of journalism.

Generally, we took a proportionate approach to dealing with specific digital issues in the code. We recognise that many of the issues raised by technology are complex and best dealt with by specific guidance such as our Guidance on AI and data protection and the AI Auditing Framework. We also considered stakeholder conversations and research about the current prevalence of technologies in the context of journalism.

The code refers to the use of social media as a source of information, and also

the challenges of correcting personal data once it starts to spread on social media. It suggests realistic steps to take, and also highlights associated guidance on social media provided by IPSO.

Throughout the code, we recognise the public interest in journalism and the pressures faced by needing to act fast. This is exacerbated by the speed of digital publication. The guidance is accordingly flexible and proportionate.

2.1.7. The special purposes exemption

The code should recognise the broad scope of the special purposes exemption for journalism, including:

- coverage of third parties who disclose personal data to journalists;
- information created in response to editorial complaints; and
- international transfers.

The code should also clearly recognise the wide margin of discretion that is given to editors when deciding what is 'reasonable' and whether data protection requirements are incompatible with journalism.

Commercial and technological developments, in particular the move online, are important. This means that recording of the use of the exemption should be flexible and proportionate to avoid becoming unmanageable in practice.

The code should avoid any inconsistencies with the description of the 'public interest' set out in industry codes.

ICO response

The code provides comprehensive guidance on the special purposes exemption. It recognises its importance as the main provision open to journalists to protect the public interest in freedom of expression and information, when data protection is judged to be incompatible with journalism.

The code explains the broad scope of the exemption in line with relevant case law. The issue of applying the exemption to complaints about stories came up a number of times, so we clarified our position on this.

As mentioned above, the code explicitly acknowledges that the exemption makes sure the independent expertise and experience of journalists is respected. Their judgement is not intended to be disregarded lightly. It also explains that journalists need to meet the relevant tests and be able to demonstrate that these legal tests are met.

We have commented above that the code includes proportionate and practical guidance about demonstrating decision-making regarding this exemption.

As also mentioned previously, we consider that the code is generally well-aligned with, and complementary to, existing industry codes.

2.1.8. Legal defences

The code should be clear about legal protection, defences and statutory exemptions which enable lawful disclosure of information to the media, as well as disclosure and publication by the media. New defences should be highlighted.

ICO response

The code explains that there are specific provisions in data protection law designed to protect freedom of expression and information where necessary. The main provision available is the special purposes exemption, but there are others. One is the condition designed to allow controllers to provide special category or criminal offence data to the media, where there is substantial public interest regarding unlawful acts and dishonesty.

The code explains the significant restrictions on the ICO's enforcement powers in the context of the special purposes and the availability of the statutory 'stay' on legal proceedings. It also sets out the public interest defences available regarding specific criminal offences under the DPA 2018.

2.1.9. Third parties

The code should reflect the high level of protection afforded to journalistic sources and the very limited legal circumstances in which details may be disclosed. Clearer guidance would be helpful about when controllers may share data with a journalist. The fear of fines may impose a chilling effect, even where there is a clear public interest.

The code should clarify responsibilities when organisations obtain information from other sources, such as:

- whistle-blowers;
- expert contributors;
- news agencies; and
- freelancers such as photographers.

Guidance about identifying controllers and processors would assist.

Guidance would also be helpful on sharing personal data with, and receiving it from, third parties securely.

ICO response

As mentioned, the code reflects the strong protection afforded to journalistic sources. We also refer to the condition under which controllers may disclose special category or criminal offence data to journalists when it meets certain requirements.

The code has a specific section on dealing with third parties and understanding the respective roles and responsibilities. This includes guidance about distinguishing between who is a 'controller' of personal data and who is a 'processor', and what this means in practice. We also discuss responsibilities when data is shared with journalists by third parties, which journalists wish to use for the purposes of journalism.

2.1.10. Supervision and review process

The code should include detail on the relationship between the ICO's regulation and other mechanisms such as self-regulation. A query was raised about how media codes would interact with sectoral codes of conduct issued under the UK GDPR.

Clarification on enforcement would be welcome, including any potential requirements to hand over devices to investigating authorities, such as computers or source documents.

There is uncertainty around the impact of other legislation or legal mechanisms on journalists such as:

- state secrets legislation;
- banning orders; or
- confidentiality or non-disclosure agreements.

It would be helpful for the ICO to review relevant adjudications and for the impact of these to be reflected as appropriate in updates to the code. The code should generally cover how it would be kept up-to-date and supervised. It could be helpful if details about the ICO's work in the area of journalism are included in the annual report.

ICO response

We explained that we consider the code is generally well-aligned with industry codes on media standards and acts as a complementary resource limited to data protection law. The code provides links to industry codes and also highlights other guidance that may be helpful on specific topics.

Under the UK GDPR, trade associations and other representative bodies may draw up codes of conduct that identify and address data protection issues

important to their members. Codes of conduct are sector-specific and are a specific accountability mechanism intended to enhance confidence in personal data processing driven by sector experience.

A draft code of conduct must be submitted to the ICO for approval and is addressed against specific criteria to make sure it meets the expected standard. A code of conduct describes the appropriate monitoring mechanisms and (where applicable) the monitoring bodies that would be accredited to monitor compliance as part of the code approval process.

The ICO is required to produce this statutory code of practice under section 124 of the DPA 2018. However, if an appropriate body wished to enhance accountability further in a relevant area, we would welcome engagement on complementary codes of conduct.

As already mentioned, the code explains the restricted application of the ICO's enforcement powers in the context of journalism.

Regarding other legislation, this code is limited to data protection legislation. However, it should be noted that a key data protection principle is that personal data must be processed lawfully. This requires consideration of any legal restrictions.

The code refers to the statutory review the ICO is required to conduct on the processing of personal data for journalism under section 178 of the DPA 2018. This is not limited to the code, but takes it into account when it is in force. We will say more about the review in due course. In the meantime, anyone open to consultation on the review can express this in the public consultation on the draft code.

2.1.11. Case studies

Case studies should be based on realistic and practical scenarios. Helpful scenarios may include:

- the 'lifecycle' of how to apply the special purposes exemption from pre-to post-publication and how you should document it;
- non-scripted TV shows;
- the relationship between data protection law, news archives and data retention;
- gathering information in public places;
- dealing with special category and criminal offence records; and
- social media.

Case studies focused on relevant legal judgements would be helpful, as would case studies focused on helping journalists strike a balance between competing rights. Rulings by IPSO were mentioned in this context.

A concern is that case studies in the code might be used too prescriptively or be too general. If the code includes case studies, principle-based examples rather than case studies that were tied too closely to specific facts are likely to be most helpful.

ICO response

We appreciate and recognise the balance to be struck between including case studies that are genuinely helpful with broader application, and adding too much detail tied to particular circumstances.

The code covers many of the scenarios mentioned above without needing to include specific case studies. We are also conscious about the availability of other industry resources and guidance for journalists to review should they wish, such as IPSO's rulings on complaints.

We thought that case studies would be most helpful where they illustrate key legal judgements impacting on the industry and which are relevant in a data protection context. This includes judgements from the broader area of privacy law, such as the tort of misuse of private information. We have chosen case law that highlights common or important areas, and which were flagged to us in this call for views. As with reference to all case law, journalists need to bear in mind that privacy law is evolving and take their own legal advice where necessary about the current position.